Low Cost and Compact Quantum Key Distribution

J L Duligall[1], M S Godfrey[1], K A Harrison[2], W J Munro[2] and J G Rarity[1]

[1] Department of Electrical and Electronic Engineering, University of Bristol, University Walk, Bristol, BS8 1TR

[2] Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS34 8QZ

E-mail: joanna.duligall@bristol.ac.uk

Abstract. We present the design of a novel free-space quantum cryptography system, complete with purpose-built software, that can operate in daylight conditions. The transmitter and receiver modules are built using inexpensive off-the-shelf components. Both modules are compact allowing the generation of renewed shared secrets on demand over a short range of a few metres. An analysis of the software is shown as well as results of error rates and therefore shared secret yields at varying background light levels. As the system is designed to eventually work in short-range consumer applications, we also present a use scenario where the consumer can regularly 'top up' a store of secrets for use in a variety of one-time-pad and authentication protocols.

1. Introduction

Quantum cryptography provides a means for two parties to securely generate shared secret material. In practice, this means that two parties can amplify an initial store of shared secrets. This shared secret may be used in three primary ways: to protect the Quantum Key Distribution (QKD) algorithm itself in order to generate new shared secrets, to identify themselves to each other, and to act as an encryption key to classically encrypt messages being sent between themselves. It is usual to delete the shared secret once it has been used. Consequently, the shared secret should be thought of as being consumable. Secrecy of the shared secret generation is safeguarded by encoding information on non-orthogonal quantum states which an eavesdropper cannot measure without disturbing. Quantum key distribution protocols are designed in such a way as to detect these disturbances and thus alert the two legitimate users to an eavesdropper's presence. Whilst QKD, in principle, is provably secure against an attacker using technology, both realistic and theoretical, experimentalists in the field are set the challenge of developing a system using current methods and apparatus whilst maintaining this ideal.

In this work we present a low cost QKD system that is aimed at protecting consumer transactions. We are willing to compromise a little on performance while retaining the high security associated with quantum protocols. The design philosophy is based on a future hand-held 'electronic credit/debit card' which communicates with consumer outlets (an Automated Teller Machine (ATM), for example) using free space optics. This device then also acts as a store of secrets shared only with the bank (or central secure server) which can be used to protect online transactions. With quantum key distribution protecting the interface between the ATM and the users handheld device, there is no possibility of an eavesdropper gaining key information via 'skimming' attacks whereby the key and card details are read using a so-called 'false front' on the ATM itself.

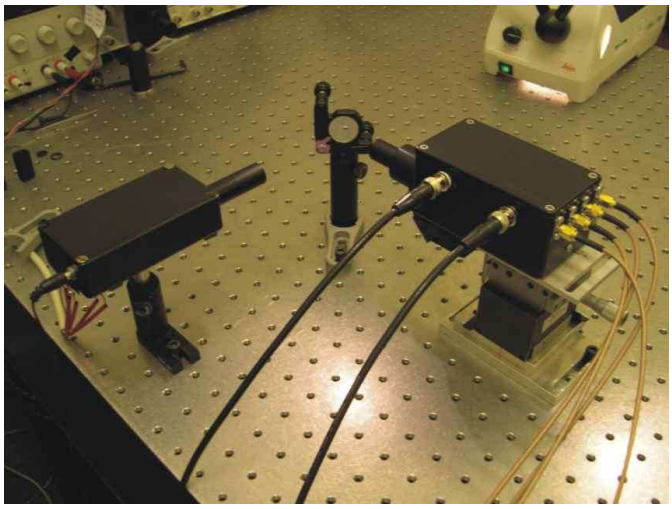

Figure 1. The quantum cryptography kit.

This paper briefly introduces the most commonly used quantum cryptography protocol devised by Bennett and Brassard in 1984 [1] since it has been implemented in the system presented. We give an overview of current research and aims in the field and then go on to outline our intended short range application. Section 2 describes the proposed system in detail focusing on how costs were brought down without compromising overly on performance. Section 3 details the experimental setup with emphasis on the purpose-built software and then presents key exchange results under various background light conditions and a security analysis of the system as a whole. Finally, the paper concludes with a discussion of the improvements needed in order to implement the proposed system within its intended application.

1.1. The BB84 Protocol

The BB84 protocol utilizes the quantum property that orthogonal polarization states can be fully discriminated and thus can be used to encode information whilst non-orthogonal polarization states cannot since measuring one necessarily randomizes the other. The protocol encodes information in the rectilinear basis (horizontal and vertical polarization) and the diagonal basis (45° and 135° polarization). The process begins with the transmitter (Alice) sending a random sequence of photons polarized in each of the four states (0° , 45° , 90° and 135°). The receiver (Bob) performs polarization measurements on the arriving photons, choosing to measure in the rectilinear or diagonal basis randomly for each photon. Alice will not know in what basis Bob measured the photons and similarly Bob is unaware of Alice's encoding basis. Once the quantum transmission is concluded, Bob announces publicly, over a classical communication channel, which photons he received and in what basis he measured them but not the actual results. Alice then replies with the instances where Bob chose the correct basis and they both discard all others. Alice will also discard all photons that Bob's detectors did not receive. If Alice and Bob use a coding scheme of 0° and 45° representing bit value 0, and 90° and 135° representing bit value 1, then the random bit string generated is the raw key. Alice and Bob's results should theoretically now be correlated unless eavesdropping has taken place on the quantum channel. The eavesdropper is required to measure photons in a random basis uncorrelated to that of Alice and then will reinject photons with errors. Eavesdropping is thus actively monitored by regularly measuring the error rate and discarding data where the error rate exceeds a certain threshold (typically $\sim 11\%$) [2].

In an experimental setup, errors will exist in the raw key because of a number of causes, including optical imperfections, background counts and detector noise. A process of error correction is therefore required and a variety of techniques are now being employed [3–6]. To minimise any information that Eve might have gained during the quantum transmission and, indeed, in the error correcting process, a further technique known as privacy amplification [7] is performed resulting in a secret key shared only by Alice and Bob. It is also usual to have both message integrity and sender authentication

on all communications over the classical channel in order to defeat a man-in-the-middle attack by Eve.

1.2. Current trends in quantum cryptography

Research in this area is focussed on several key factors. The most obvious areas for improvement are transmission range and rate. Long distance free-space QKD experiments have developed to the extent where a 23km key exchange at night was carried out by Kurtsiefer *et al* [8] in 2002. Significant progress has been made in daylight QKD operation, initially by Jacobs and Franson in 1996 [9] and later by Buttler *et al* [10] in 1998. The current record is a 10km link achieved by Hughes *et al* in 2002 [11]. A study has also taken place suggesting that there are no technical obstacles in developing a quantum key distribution system between ground and low earth orbit satellites [12]. Systems using optical fibre as the transmission medium have achieved greater distances with Gobby *et al* [13] achieving key exchange over 122km. As far as transmission rate is concerned, several systems are now operating at giga-hertz clock rates [14, 15].

Improving current technologies is imperative for quantum cryptography's future. Producing detectors with greater efficiency as well as moving away from faint pulsed lasers as approximations to single photons will eradicate many security worries. Improvements in the reliability and efficiency of true single photon sources are being made with encouraging results [16]. QKD systems are now being sold as commercial products. MagiQ Technologies ‡, IDQuantique§ and SmartQuantum‖ all offer fibre-based systems for sale whilst other organisations such as QinetiQ, Toshiba and NIST have quantum cryptography capabilities. The systems currently available are expensive, use purpose-built components and are made-to-order. Moreover, their market base is primarily organisations such as the military, financial services or high intellectual property establishments. The work presented in this paper is a clear departure from this goal. It represents a ground-up approach to quantum cryptography, exploring the possibilities of bringing secure electronic communication and data exchange to the consumer. This research forms part of the SECOQC network¶ and concentrates on that final link in the chain from network to consumer/end user by providing end-to-end security for the user as well as the channel.

1.3. The Application

Figures of credit card fraud loss in the UK for 2004-2005[+] show that the only type of fraud to increase this past year was so called 'CARD-NOT-PRESENT' crime typical of mail order or online transactions. Here we propose a method of protecting these

‡ www.magiqtech.com
§ www.idquantique.com
‖ www.smartquantum.com
¶ www.secoqc.net
[+] www.apacs.org.uk

transactions using the shared secret stored in a personal handheld transmitter which is regularly topped up by secure key exchange with a stationary receiver unit. The Alice module would be incorporated within a small device such as a mobile phone, or PDA, and the Bob module within a large fixed device such as a bank ATM, known as the "Quantum ATM".

A typical usage scenario would be for a customer to register for this service in her bank. Once the customer is verified as a legitimate account holder, she is given a SIM card (or an equivalent storage device) containing an initial unique secret bit string which she shares with a central secure server that all ATMs have access to. This One-Time-Pad (OTP) is then used to authenticate and encrypt future transactions, whether it be withdrawing cash from an ATM or buying products online. As each security operation requires the consumption of some of the shared secret, the user would periodically revisit the "Quantum ATM" and 'top up' both their copy and the Bank's copy of the shared secret.

2. The System

The system described here is based on the BB84 protocol with a slight variation from the usual free space experimental implementation. Figure 2 shows a common optical arrangement in a receiver unit where the random basis selection and polarization measurement is made. For example, a vertically polarized photon, emitted from Alice is directed through the 50:50 beamsplitter BS, making the basis selection. If it is reflected, the photon is to be measured in the rectilinear basis and the polarizing beamsplitter PBS_1 directs the photon to a detector according to its polarization. Thus D_1 receives a click. If the photon is transmitted at BS, the diagonal basis is chosen and the photon passes through the $\lambda/2$ plate and then PBS_2 where, in the case of a vertically polarized photon, either D_3 or D_4 might click with equal probability. This result would be discarded later in the sifting process as Bob measured the photon in the wrong basis. Therefore, in general, the BB84 implementation has a 50% protocol efficiency as half the photons will be measured in the wrong basis. We use a different optical arrangement which acts to reduce the size of the module as well as the cost. It involves the use of a holographic diffraction grating to produce a 2x2 matrix of beam paths (figure 2). The grating therefore makes the random basis selection by sending an incident photon in one of four directions. In order to make the polarization measurements in accordance with the BB84 protocol, dichroic sheet polarizer was placed in front of each detector in one of the four polarization orientations. Note that in this arrangement, the protocol efficiency has dropped to 25% since the photon is directed randomly in one of four ways. This trade-off in efficiency vs. cost was deemed acceptable since there are far fewer transmission losses in a short range system.

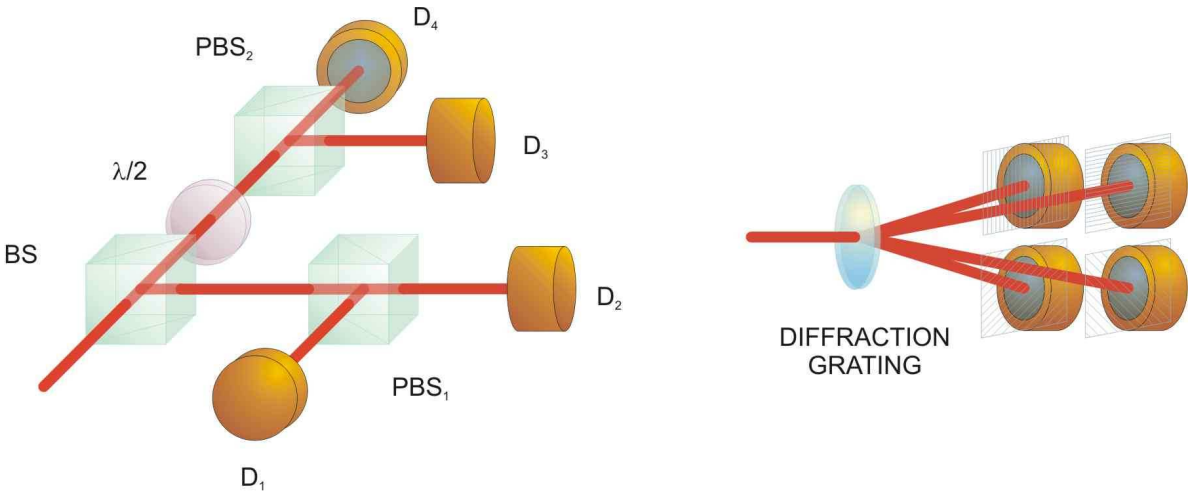

Figure 2. On the left, a common implementation of the BB84 protocol using a beamsplitter cube (BS), a half-wave plate ($\lambda/2$) and two polarizing beamsplitter cubes (PBS_1 and PBS_2). The diagram on the right shows a compact system using a diffraction grating and dichroic sheet polarizer over each detector.

2.1. The Alice Module

In its experimental form, the Alice module uses off-the-shelf IC components in a driver circuit which produces sub-5ns pulses. The driver pulses are then ANDed with the output from a digital input/output card (NuDAQ, *Adlink* PCI-7300A) and passed to one of four AlInGaP, miniature, red-orange LEDs (*Agilent*, HLMA-QH00), see figure 3. The output from the NuDAQ card is regulated by an external oven-stabilized clock (*C-MAC Frequency Products*, CFPO-6) and passes a random bit string, generated by a quantum random number generator (QRNG), (*IDQuantique*, Quantis) to the Alice module, recording which LED fires. Due to the limitations of the i/o card, the driver pulses are produced at a repetition rate of 5MHz. The four LEDs were intensity balanced by adjusting the current to each diode and timing jitter measurements were carried out for each channel showing, on average, pulses of $2.4ns$ duration. Figure 3 also shows the resulting time interval histogram of one channel.

The LEDs are attached to a holder, see figure 4, with dichroic sheet polarizer, orientated in each of the four polarization states, $0°$, $45°$, $90°$ and $135°$, placed over each output. To combine the beam paths, the same four way diffraction grating arrangement was used. The holder serves to direct the polarized light towards the grating as well as restrict the viewing angle of the diodes. A pinhole was placed after the grating together with a 50mm focal length lens to collimate the beam. A $632.8 \pm 3nm$ filter was included to limit the bandwidth.

Alice and Bob communicate via the internet. This is assumed to be a public channel. In the intended use model, this will be replaced by an IrDA infra red communication channel.

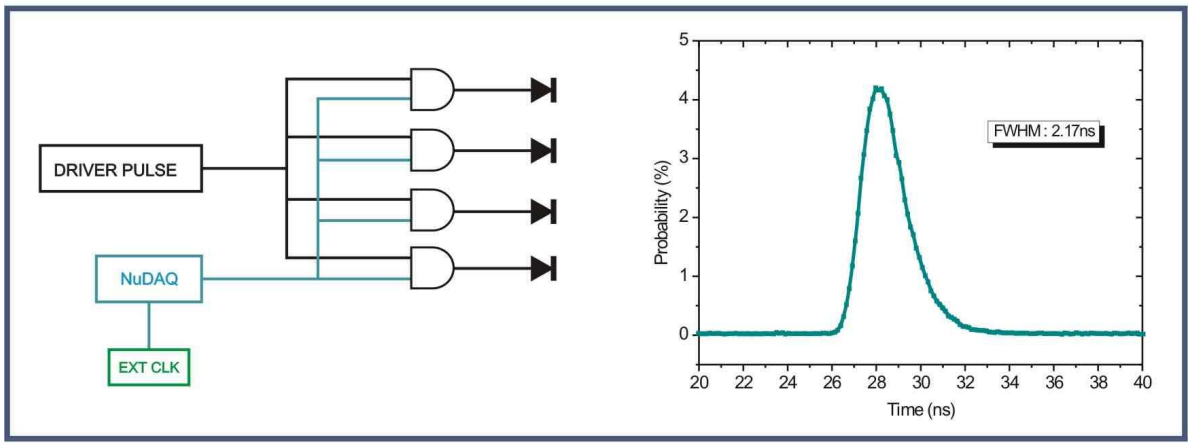

Figure 3. The sub-5ns driver pulse is ANDed with the signal from the digital I/O card (NuDAQ) that determines which LED will fire. The time interval histogram gives a measure of the optical pulse width of one LED from the Alice module.

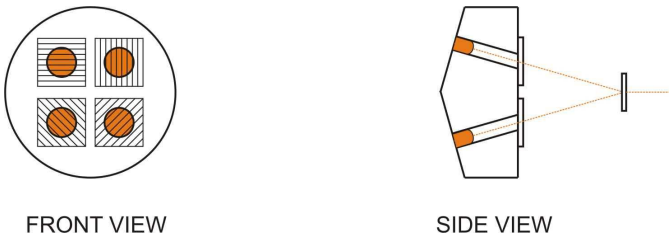

Figure 4. Front and side view of the holder designed to house the LEDs. The front view shows the dichroic sheet polarizer placed over each LED output.

2.2. The Bob Module

In its experimental form, the Bob module contains four passively quenched silicon avalanche photodiodes (*Perkin Elmer*, C30902S) which are cooled down to -10° C and maintained by a temperature controlling circuit. Since these detectors operate at a relatively high voltage, a high voltage DC-DC converter (*EMCO*, Q03-5) was included so that the Bob module can run off a low voltage supply. A simple discriminator circuit takes the output from the detectors and converts it to a readable positive pulse. Time of arrival information is recorded by a time interval analyser card (TIA, *GuideTech*, GT653).

In a similar setup to the Alice module, the dichroic sheet polarizer was placed in front of each detector orientated in the four polarization directions with the diffraction grating in place, as shown in figure 2. In addition to this arrangement, a $632.8 \pm 3nm$ filter was included to reduce the background count and a 50mm focal length lens to collect the beam from Alice and focus it down onto the detectors.

The bit error rate (BER) for each channel was estimated from data taken during key exchange (see section 3).

$$BER = \frac{N_{wrong}}{N_{total}} \tag{1}$$

where N_{wrong} is the number of bits in error and N_{total} is the number of bits received in total.

This gives a measure of the likelihood of Bob receiving a 0 when a 1 was sent from Alice. All but one of the BER values in table 1 are sufficiently low showing that optical imperfections from the equipment will contribute little to the error in the sifted key. Unfortunately, the over-sensitivity of one detector in the Bob module is responsible for the greater BER in the 135° channel. Whilst this problem does increase the overall base error rate of the system and ultimately bias Bob's data opening it up to possible attacks [17], this was deemed acceptable with the current set of equipment providing proof-of-principle results. An updated version of the receiver module is in development with balanced detectors and a more efficient cooling system to lower the dark count rates.

Table 1. Table showing the BER values at 0°, 45°, 90° and 135° as percentages calculated from equation 1.

Channel	Bit Error Rate (%)
0°	1.32
45°	2.54
90°	2.20
135°	4.75

2.3. Loss Tolerance of a Daylight System

Since the module will have to be able to operate in daylight conditions, the background error rate [12] is the most important consideration in designing the receiver unit. It will be the limiting factor of the entire system.

The signal count for this system is defined as

$$S = \frac{RMT\eta}{4} \tag{2}$$

where R is the pulse repetition rate, M is the average number of photons per pulse, T is the lumped transmission (including geometric loss) and η is the detection system efficiency. The protocol effectively splits the signal into four on the detectors leading to a factor of 4 reduction in signal bit rate after sifting the key. The background rate is given by

$$P_b = Bt \tag{3}$$

where B is the background count rate per detector and t is the time synchronization gate. Half these background counts induce an error and half are thrown away in the protocol but contributions arise from all four detectors.
Using equations (2) and (3), the background error rate is thus given as

$$E = E_{base} + \frac{P_b}{S} \tag{4}$$

A base error rate of $E_{base} = 0.027$ (derived from an average of the values in table 1) is expected thus

$$E = 0.027 + \frac{4Bt}{MT\eta} \tag{5}$$

Error correction schemes will operate efficiently with an error rate of $E < 0.08$, therefore the maximum acceptable background count rate per detector is given as

$$B < \frac{MT\eta}{75.5t} \tag{6}$$

In considering the system presented here, estimates can be made for the following values:

- $M \sim 0.3$, an accepted value for guaranteed security of low loss systems, using the optimal choice for the expected photon number taken from [18].
- $T \sim 1$ since the source can be imaged onto the receiver and the system is short range and thus atmospheric loss is negligible.
- $\eta \sim 0.045$ taking into account the quantum efficiency of the detectors and the presence of the narrowband filter and polarizers.
- $t = 5ns$ gate synchronization time.

Thus the maximum background count rate per detector can be given as roughly

$$B \leq 36000 \text{ Counts/sec}$$

The current version of the Bob module can operate in shaded areas but not in full direct sunlight. Of course higher error rates are in part due to a relatively wide time synchronization gate. This is due to the limitation of using LEDs to produce short pulses. The timing window can be shortened further but then the bit rate is reduced, as is shown in section 4, figure 9. An updated version is under development whereby a

restriction in the field of view and greater spectral filtering will be introduced. Shared secret generation has been carried out at background light levels of up to 26000 counts/sec and the results are shown in section 3.

In order to ascertain how well the hardware compared to equation 5, a random data string was sent from Alice to Bob and the percentage of errors at varying backgrounds was calculated. Figure 5 shows this relationship as well as the predicted error rate for each background level. The dashed red lines are essentially an upper and lower bound to the predicted error rate since the channels within the Bob module have slight differences in efficiency. As is shown, the data points all fit well within these bounds. Again, an updated version of the Bob module is expected to increase the value of η to about 0.08 per detector and thus raise the background level at which the system can operate to over 60000 counts per second. Also note that our two channel measurement system (see section 3.1) effectively doubles the background rate per detector and a four channel measurement system will further improve our resilience to background light.

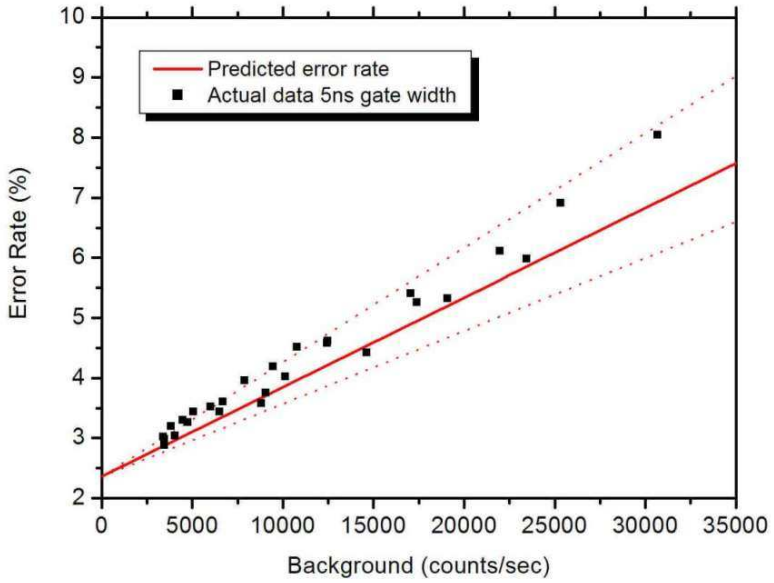

Figure 5. Graph showing the relationship between the estimated error rate and the background counts per second The red line is the predicted error rate calculated from equation 5. Our current Bob module has detectors of slightly varying detection efficiency. The dashed lines indicate the predicted error rate with η at 0.045 and 0.055.

3. Experimental Setup

The experimental setup for quantum key distribution is shown in figure 6. As mentioned in section 2.1, a file containing a random bit string generated from the QRNG is supplied to the NuDAQ which in turn controls the Alice module at a repetition rate of 5MHz.

The quantum transmission is received by the Bob module which passes the four channel outputs to the TIA card.

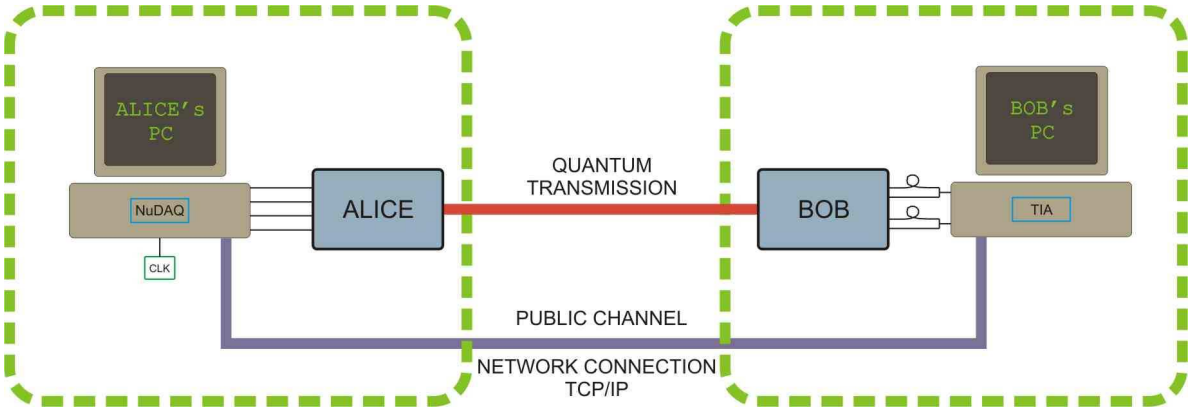

Figure 6. Schematic showing the experimental setup for demonstrating key exchange.

3.1. Software

The key requirements from the software is that it should be fast establishing a key within seconds. This should work with minimal interactivity between Alice and Bob and with low processing power at Alice. The synchronization (of both clock and start time) and error correction software have been developed with these constraints in mind.

3.1.1. Synchronization In this system, the data is recorded first during the quantum transmission and processed afterwards in a few seconds. The start of the transmission is determined approximately by searching for a jump in the frequency of time tags as Bob starts measuring before Alice begins her transmission. Alice transmits sub-$5ns$ pulses every $200ns$, therefore a time synchronization gate of $5ns$ reduces the probability of registering a background event within the gate by a factor of 40. The clock at Bob is thus synchronised with the clock at Alice by searching for time tags that sit at separations of $200ns$ and adjusting the time separation slightly every $\sim 100ms$ to compensate for clock drift. The advantage of this setup is that no timing reference signal is needed. To determine the exact start time of the data Bob reveals a random subset of his measured bit values and the basis he used to Alice. Alice then finds the data start by performing a sparse correlation against her stored data. This random subset can also be reused to estimate the error rate.

Since the GT653 is a two-input card, we combine two channels into one input by delaying one channel by $40ns$, see figure 7. In doing this, the background count rate is effectively doubled. This is not currently a problem since we can determine the true signal to noise ratio from the data and calculate error rates and thus secret bit yields against this background. However, the background count rates shown are not per detector but per channel and so using the TIA card in this manner does become

a limiting factor when operating at higher background light levels as we are effectively making the situation worse. Improvements to this setup are discussed in section 4.

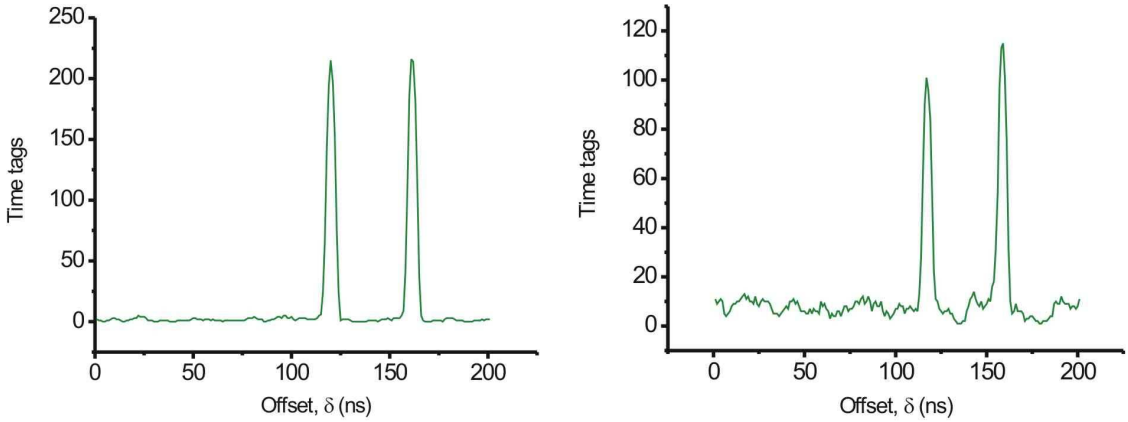

Figure 7. Two histograms showing the results of running the synchronization routine on the data from the TIA card. The card has only two input channels so two channels from Bob are coupled onto the other two with a fixed delay of $40ns$ accounting for the two peaks shown. The right hand graph shows how the noise increases when the experiment is run in higher background light levels.

3.1.2. Error correction Most quantum cryptography systems use the Cascade [3] algorithm since it operates close to the theoretical Shannon limit. It is highly interactive involving many separate two-way communication steps. Any latency in the classical channel dramatically slows the process. Thus another method of error correction has been adapted for this system. We have chosen a version of the Low Density Parity Check (LDPC) [19] algorithm as the protocol has very little interactive communication. In fact, Alice merely needs to transmit an error correction syndrome to Bob. One drawback is that LDPC requires a pessimistic lower bound estimate of the error rate. The synchronization protocol already provides us with an error estimate. Information revealed during the error correction process is removed by a privacy amplification process [7] in which key length is reduced.

It should be noted that our implementation of error correction requires that Alice and Bob both generate the same random factor graph. Once Alice and Bob know the number of message bits they are error correcting over, and the measured error rate, they seed a pseudo random number generator from their OTP and use this to generate an appropriate factor graph. Eve, the eavesdropper, is assumed not to know which of the 2^{256}, say, different factor graphs Alice and Bob are using.

3.2. Experimental Results

Using the experimental setup described in section 3, we carried out a series of key exchange runs at varying background light levels. From the data we extracted an

error rate using the methods described above. The error corrected keys were then passed through the privacy amplification process to remove all possible information leaked to a theoretical eavesdropper. This effectively reduces the length of the key but ensures absolute secrecy. To estimate the key length reduction, we use the Lutkenhaus bound [20] and details are presented in the appendix. The resulting number of bits divided by the collection time thus gives us an equivalent secret bit rate as a function of background counts which we show in figure 8. We are able to establish just over 4000 secret bits per second at low background with over 500 secret bits at count rates exceeding 25000 counts/sec. We note here that we have maintained a very pessimistic view of the eavesdropper's capabilities and there may be the possibility of increasing the number of secret bits without incurring too strong a security penalty. Our near term target will be to improve the system to the point where 10000 secret bits can be generated even with backgrounds of order 30000 per second. We can immediately do this if we double the repetition rate to 10MHz, improve the Bob module detection efficiency to 8% and increase the protocol efficiency from 25% to 50%. We discuss this further in the following section.

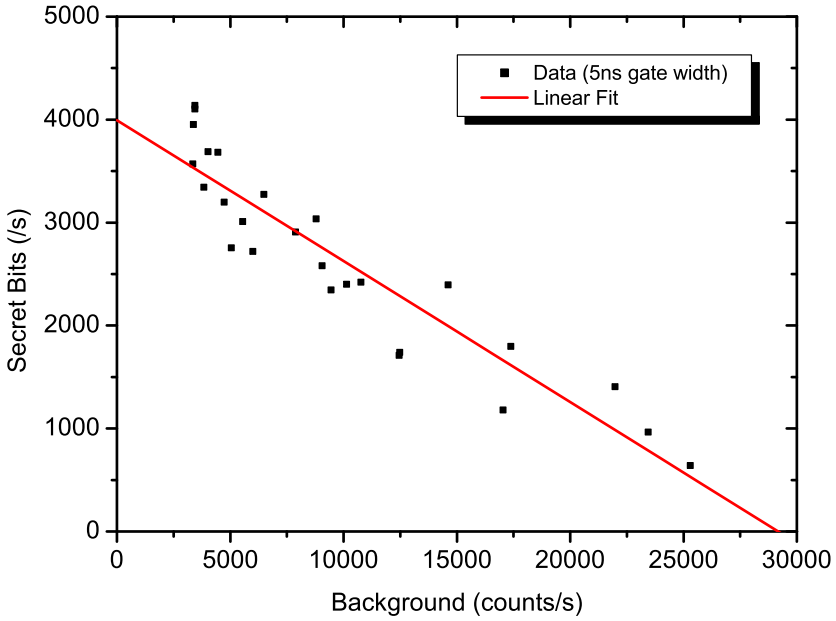

Figure 8. Graph showing the relationship between the secret bit rate and the background counts per second.

4. The Future

The initial experimental setup has shown that off-the-shelf components can be used to carry out quantum key distribution. We are currently working to produce stand-alone

modules for the transmitter and receiver. An inexpensive Field Programmable Gate Array (FPGA) will be used to replace much of what has been achieved by software on Alice's computer as well as replace the driver circuit shown in section 2.1. The transmission rate of this system will be increased to 10MHz. We will interface the FPGA Alice module with a PDA (*Hewlett-Packard*, iPAQ hx4700 series) via serial cable and are developing the software to run on the PDA which will incorporate the IrDA or BlueTooth facilities as the QKD public channel. We are also working on an FPGA solution to the time interval analyser on the receiver side. A four channel TIA module with an estimated resolution of $300ps$ is under development.

Improvements to the software both in speed and efficiency are under way. There are plans to dynamically evaluate Bob's data using various time synchronization gate widths depending on the level of background counts. In this way we will still be able to obtain secret bits at higher background levels. It is important that we do not waste the OTP stack by authentication protocols whilst attempting to carry out key exchange in very bright conditions. Once the OTP is depleted from too many unsuccessful attempts to extend the key, the user would have to revisit the bank to obtain a new OTP. Figure 9 illustrates how a secret bit rate can be achieved at higher background count rates by evaluating Bob's data with narrower gate widths.

On the hardware side, we plan to improve the Bob receiver module. Initially we will start by using an improved grating and polarizers to increase the efficiency to around 8%. However, as the receiver module can be a static medium cost device, it may prove better to return to a classical beamsplitter based design with protocol efficiency of 50%. Eventually the Alice module must be able to be brought to the Bob module and fully automatically aligned. Initially this may be simply done using a fixed alignment cradle or docking station. However, we are also considering active methods for aligning a hand-held Alice module to a stationary Bob module.

5. Conclusion

We have built a low cost free-space quantum cryptography system using off-the-shelf components that is able to generate and renew shared secrets on demand over a short range of up to a metre in shaded daylight conditions. The transmitter unit is compact and we are aiming eventually to incorporate it in a hand held device such as a smart card or mobile phone. A full software system has been developed to handle synchronization, error estimation and correction and privacy amplification. We have tested the system in a range of background levels up to that equivalent to shaded daylight conditions. The system is designed to work in short-range consumer applications and we have described a use scenario where the consumer can regularly 'top up' a store of secrets for use in a variety of one-time-pad and authentication protocols. We have described various improvements to the system that will increase our background light tolerance and bit rates while reducing cost and complexity. Currently, our system can generate around 4000 bits of secret keys from a one second interaction between transmitter and receiver

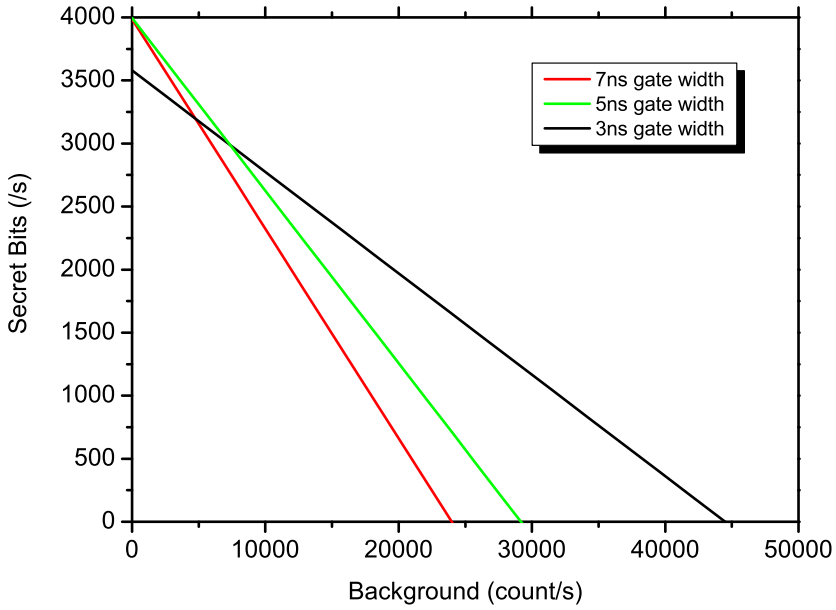

Figure 9. Graph showing the relationship between the secret bit rate and the background counts per second using 3,5 and 7ns time synchronization gate widths. Since the system must be able to operate in daylight conditions there could be a procedure whereby Bob samples the background count before synchronization and correlation procedures and chooses which gate width to use.

in low light conditions. In the next generation device we expect to be able to operate at 10000 secret bits per second up to full daylight conditions.

6. Acknowledgements

We gladly thank Alastair Lynch from the University of Bristol for his continued work on this project. John Rarity acknowledges support from the Royal Society through a Wolfson Research Merit Award. Mark Godfrey is funded by EPSRC CASE studentship through QinetiQ. Joanna Duligall is funded by EPSRC CASE studentship through HP Laboratories. This work has also been supported by the EU under project number FP6-2002-IST-1-506813 SECOQC and we would also like to acknowledge the EPSRC QIP IRC for their support.

References

[1] C.H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, pages 175–179, 1984.

[2] Peter Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000.

[3] Gilles Brassard and Louis Salvail. Secret key reconciliation by public discussion. In T. Helleseth, editor, *Proceedings of Advances in Cryptology - EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 1993*, volume 765 of *Lecture Notes in Computer Science*, page 410. Springer-Verlag GmbH, 1994.

[4] A Yamamura and H Ishizuka. Error detection and authentication in quantum key distribution. In Mu Y Varadharajan V, editor, *6th Australasian Conference on Information Security and Privacy SYDNEY, AUSTRALIA, JUL 11-13, 2001 Informat & Network Syst Secur Res, Macquarie Univ, Australian Comp Soc, Univ Western Sydney*, volume 2119 of *LECTURE NOTES IN COMPUTER SCIENCE*, pages 260–273. SPRINGER-VERLAG BERLIN, BERLIN, May 2001.

[5] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*, 67(5):052303, May 2003.

[6] D. Pearson. High-speed qkd reconciliation using forward error correction. In *The Seventh International Conference on Quantum Communication, Measurement and Computing*, pages 299–302, 2004.

[7] C.H. Bennett, G. Brassard, and J-M. Robert. Privacy amplification by public discussion. *SIAM Journal of Computing*, 17(2):210–229, April 1988.

[8] C. Kurtseifer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, and J.G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419:450, October 2002.

[9] C.B Jacobs and J.D Franson. Quantum cryptography in free space. *Optics Letters*, 1854-1856(22):3, 1996.

[10] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, C. G. Peterson J. E. Nordholt, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Physical Review Letters*, 81(15):3283–3286, 1998.

[11] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson. Practical free-space quantum key distribution over 10km in daylight and at night. *New Journal of Physics*, 4:43.1–43.14, July 2002.

[12] P.M. Gorman J.G. Rarity, P.R. Tapster and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4:82.1–82.21, October 2002.

[13] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(3762-3764):14, December 2004.

[14] Karen J. Gordon, Veronica Fernandez, Gerald S. Buller, Ivan Rech, Sergio D. Cova, and Paul D. Townsend. Quantum key distribution system clocked at 2 ghz. *Optics Express*, 13(8):3015–3020, April 2005.

[15] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, Charles W. Clark, Carl J. Williams, E. W. Hagley, and Jesse Wen. Quantum key distribution with 1.25 gbps clock synchronization. *Optics Express*, 12(9):2011–2016, May 2004.

[16] R Alléaume, F Treussart, G Messin, Y Dumeige, J-F Roch, A Beveratos, R Brouri?Tualle, J-P Poizat, and P Grangier. Experimental open air quantum key distribution with a single photon source. *New Journal of Physics*, 6(92), July 2004.

[17] V. Makarov and D.R. Hjelme. Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 5:691–705, 2005.

[18] N. Lutkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61:052304–1–10, 2000.

[19] R.G. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, pages IT–8:21–28, 1962.

[20] N. Lutkenhaus. Estimates for practical quantum cryptography. *Physical Review A*, 59:3301–3319, 1999.

Appendix

The number of sifted key bits received in a transmission of duration t is given by

$$n_{rec} = St \tag{A.1}$$

In using the LDPC coding scheme, the error correction efficiency E is calculated using

$$E = 1 - n_{syn}/n_{rec} \tag{A.2}$$

where n_{syn} is the number of syndromes needed. Maintaining a pessimistic view of an eavesdropper's capabilities, we discard all syndrome bits. In considering a pulse splitting attack with zero loss transmission technology [20], the eavesdropper takes all the pulses at the output of Alice an blocks all single photon pulses. Multi-photon pulses are split and sent on through a loss free channel to Bob. The split off photons are stored until the bases are revealed thus making all received pulses insecure. If we assume a Poisson distribution for the faint pulse photon number probability then

$$P(n) = \frac{M^n e^{-M}}{n!} \tag{A.3}$$

and

$$P(n \geq 2) = 1 - e^{-M} - Me^{-M} \tag{A.4}$$

Secret bits are only gained when the received photon rate n_{rec} is greater than the multi-photon rate. We then calculate the fraction of received bits that are guaranteed to be secure as

$$b = 1 - \frac{(1 - e^{-M} - Me^{-M})}{(1 - e^{-M})T} \tag{A.5}$$

where T is the efficiency of the free space channel.

We cannot use these bits either in the key or to estimate the error rate. Hence using Lutkenhaus' formulae, the secret bit rate becomes

$$n_{fin} = (n_{rec} - n_{err})b\left(E - log_2\left(1 + 4\frac{\epsilon}{b} - 4\left(\frac{\epsilon}{b}\right)^2\right)\right) - n_s \tag{A.6}$$

where n_{err} is the number of bits used to estimate the error, ϵ is the estimated error rate and n_s is a safety margin in this case set to 100 bits.
Calculating n_{fin} for each data point, figure 8 shows how the secret bit rate varies with background count.